REMARKS/ARGUMENTS

Claims

The Examiner rejected claims 1-8. By this amendment, claim 1 has been amended. Therefore claims 1-8 remain pending in the application.

Claim Rejections – 35 USC §102

Claims 1-2 were rejected under 35 USC 102(e) as being anticipated by Debry (US Pat. No. 6, 314,521) (hereinafter Debry ['521]). The rejection is respectfully traversed.

Regarding claim 1 the Examiner stated that Debry ['521] discloses at col. 8, line 65 to col. 9, line 14: "authenticating the printer to the server by comparing the secret unique identifier installed in said printer and said server, using a secure transmission over said network." However, those lines of Debry ['521] in fact do not directly compare a secret unique identifier. Instead, those lines of Debry ['521] only indirectly compare a unique key stored at both a printer and at a certificate authority. In Debry ['521] the printer sends an encrypted message to the certificate authority and the certificate authority decrypts the message using the certificate authority's encryption key. The certificate authority then knows that only a specific printer could have encrypted the message with the unique key stored at the certificate authority. According to Debry ['521], a printer never sends a secret encryption key to a server, and a server never recovers a secret encryption key from data received from a printer.

In the present invention, a printer transmits a secret unique identifier directly to a server, securely encrypting the secret unique identifier using a session key. To make this process more clear, claim 1 has been amended to add the explicit step of "transmitting the secret unique identifier from the printer to the registration server and receiving the identifer in the registration server using a secure transmission over said network." Such a step is neither disclosed nor fairly suggested in the teaching of Debry ['521].

Support for the above limitation is found in the present Fig. 50 and in the specification at page 49, line 26 to page 50, line 4: "A preferred embodiment of a printer registration protocol is shown in Figure 50. According to the protocol, when the printer connects to the netpage network for the first time after installation, it creates a signature public/private key pair 91,92. It transmits the secret ID and the public key 91 securely to the

netpage registration server 11. The server compares the secret ID against the printer's secret ID recorded in its database 74, and accepts the registration if the IDs match. It then creates and signs a certificate containing the printer's public ID and public signature key, and stores the certificate in the registration database. The printer stores its private key 92 in its flash memory 81."

The applicant asserts that the rejection of claim 2 is now moot as claim 2 is dependent on claim 1.

Claim Rejections – 35 USC §103

The Examiner rejected claims 3-8 under 35 USC 103(a) as being unpatentable over Debry ['521] in view of Debry (U.S. Pat. No. 6,385,728) (hereinafter Debry ['728]). The rejection is respectfully traversed.

Regarding claim 8, the Examiner states that Debry ['521] discloses at col. 8, lines 56-64: "A network registration signal for transmission over a network from a printer to a remote registration server to register the printer with the server, where the signal is transmitted at the first occasion the printer is connected to the network, and includes: a secret unique identifier and a public unique identifier retrieved from non-volatile memory in the printer." However, the applicant asserts that the above lines of Debry ['521] in fact do not disclose including a secret unique identifier in a network registration signal. Rather, those lines of Debry ['521] state in part that "Using the encryption key built in at manufacturing time, the printer 20 encrypts a message containing the printer's model number, serial number, and IP address. It then appends to this, in the clear, the model number and serial number, and sends this message to the certificate authority." Note the there is no mention in those lines of Debry ['521] of including the encryption key itself in the message.

Similar to the argument presented above with respect to claim 1, the applicant asserts that the Examiner improperly equated the indirect comparison of two secret encryption keys as disclosed in Debry ['521] with the direct comparison of secret unique identifiers that is recited in claim 8.

Regarding the rejections of claims 3-7, the applicant asserts that the rejections are now moot in light of the arguments presented above concerning claim 1, as claims 3-7 are all dependent on claim 1.

Conclusion

Independent claim 1 has been amended to explicitly include the step of transmitting a secret unique identifier from a printer to a registration server. Based on the arguments given above, the Examiner's rejections of independent claims 1 and 8 are respectfully traversed. Accordingly, it is submitted that the application is now in condition for allowance. Reconsideration and allowance of the application is courteously solicited.

Very respectfully,

Applicant: _____

PAUL LAPSTUN

Applicant: _____

KIA SILVERBROOK

C/o: Silverbrook Research Pty Ltd
393 Darling Street
Balmain NSW 2041, Australia

Email: kia.silverbrook@silverbrookresearch.com

Telephone: +612 9818 6633

Facsimile: +61 2 9555 7762